Primary and Secondary Control as Antecedents to the Dark Traits in Predicting Attraction to Hacking Behavior

Laura Amo
University at Buffalo

Joana Gaia
University at Buffalo

David Murray
University at Buffalo

G. Lawrence Sanders
University at Buffalo

Sean Patrick Sanders
University at Buffalo

Shambhu Upadhyaya
University at Buffalo

Xunyi Wang
Baylor University

The current study examines the relationship between the need for control, the Dark Triad personality traits, and hacking intent. We surveyed 523 individuals using a scenario design and investigated the role of both primary and secondary control as antecedents to Machiavellianism, psychopathy, and narcissism leading to both white- (i.e., ethical) and black-hat hacking interest. Our findings suggest that primary control is a significant antecedent to all three dark personality traits such that a higher intrinsic need for control is positively associated with Machiavellianism, narcissism, and psychopathy. Secondary control, however, has comparatively different effects on dark personality traits, demonstrating a negative effect only on psychopathy. Both Machiavellianism and psychopathy predicted both white- and black-hat hacking interests along with the perceived probability of apprehension. Overall, our findings suggest that primary control drives all three dark personality traits, yet only two of the three dark personality traits – Machiavellianism and psychopathy – are related to hacking interest.

Keywords: black hat, Dark Triad, hacking, insider attacks, primary and secondary control, white hat

INTRODUCTION

The United States Cybersecurity and Infrastructure Security Agency (CISA) defines an insider as "any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems" (Chickowoski 2018). A substantial portion of privacy violations can be traced to insiders, including funds embezzlement, pilfering of trade secrets, customer information theft, competitive information, and related fraudulent activities (Robert Willison 2018). The emergence of the virtual organization has expanded our notion of insiders to include current and former employees, contractors, consultants, board members, outsourced network engineers, software developers, product designers, logistics, sales, vendors, and maintenance services. Losses from insider attacks can be significant, as the average cost of an insider attack approaches $8 million (Chickowoski 2018).

The ongoing COVID-19 pandemic has stressed employees and organizations, fueling the already out-of-control fire concerning security threats. The healthcare industry forecasted increased cyber-criminal activity during the COVID-19 pandemic (Weston 2020). On the other hand, social engineering attacks attributed to the coronavirus pandemic turned out to be the most significant security threat faced by the public and private sectors (Hijji and Alam 2021). This increase in insider breaches may be traced to the shift to remote work, employee feelings of job insecurity, and increased access to cloud-based data. Surprisingly, the mass transition to remote work created significant angst for security professionals (Pranggono and Arabo 2021).

Although psychological profiling of hackers has attracted substantial research interest, the empirical results are limited (Crossler et al. 2013; Dhillon et al. 2016; Kajtazi et al. 2014; Roy Sarkar 2010; Safa et al. 2018; Warkentin et al. 2016), and researchers are still learning about the precursors to different types of hacking behavior.

PSYCHOLOGICAL RESEARCH ON HACKERS

White hat hackers or ethical hackers (Palmer 2001) assist system owners in detecting and fixing security system vulnerabilities. They do not violate laws, even though many use the same tools as black hat hackers. Black hat hackers or crackers are typically motivated by personal gains, including financial gains, from illegally breaching computer systems (Krit and Haimoud 2016). However, they can be social mischief-makers seeking thrills, revenge, and notoriety.

Within the emerging research on hacking behavior, the Dark Triad (or dark traits) has received considerable attention from cybersecurity researchers because it is considered an influential antecedent to unethical behavior in general (Pelster et al. 2021). Dark traits are prevalent in the population and even more so in the corporate environment (Pelster et al. 2021). The Dark Triad personality traits consist of *Machiavellianism* (manipulative, deceitful, and exploitive), *narcissism* (self-centered and attention-seeking), and *psychopathy* (lack of remorse, cynical, and insensitive) (Jonason and Webster 2010; Paulhus and Williams 2002). There is a fair amount of overlap among the dark traits such that there tend to be positive intercorrelations within individuals; for example, those high in psychopathy tend to be high in narcissism and Machiavellianism (Bertl et al. 2017) (Muris et al. 2017). For these reasons, the traits are often studied concerning deviant behavior and outcomes.

Although research is still emerging on the role of the Dark Triad in developing a hacker persona, some existing research indicates that some or all of the Dark Triad personality traits predict hacking intent or feelings about hacking. For example, a study involving 474 subjects found that white, grey, and black hat hackers scored high on the Machiavellian and psychopathy scales (Gaia 2021). Another recent study found relationships between the Dark Triad and techniques for hacking. Specifically, individuals high in Machiavellianism used stealthy network discovery and scanning strategies for hacking, whereas individuals high in psychopathy and narcissism, in comparison, used less stealthy discovery and scanning strategies (Jones et al. 2021). Finally, in another study, Maasberg et al. surveyed 768 IT professionals on Amazon Mechanical Turk. The researchers found that persons higher on Machiavellianism, narcissism, and

psychopathy were more sympathetic towards individuals who breached employee privacy by posting salary information of higher-paid coworkers (Maasberg 2020). Overall, the emerging literature in this area suggests that dark traits, particularly Machiavellianism, are associated with certain types of hacking.

CONTROL THEORY

Control is a driving force in behavior, and individuals strive to produce behavior-event contingencies to exert primary control over the environment (White 1959). Theories of control assume that individuals attempt to control their environment and directly manage personal development (Wrosch et al. 2000) by setting goals, seeking their attainment, and dealing with the negative consequences over their lifetimes (Heckhausen 2006). Some researchers have posited that persons high on dark traits tend to act out due to a perceived lack of control over their environment (Aldoursari and Ickes 2021).

Similar arguments have been made concerning cybercriminals. Regarding cybersecurity, researchers (Rennie and Shore 2007) posit that hackers are partly motivated to gain control of a portion of their lives, deal with unresolved anger, and crave media recognition. Indeed, hackers report feelings of control when concentrating and applying their skills and achieving favorable outcomes (Rennie and Shore 2007). Likewise, hackers tend to *reject* external control of their behavior. For example, sanctions are supposed to deter individuals from breaking the rules. Yet, black hat hackers regularly ignore the threat of sanctions (Silic and Lowry 2021), turning to criminal behavior to realize unmet personal financial and social goals by exercising control over their environment by hacking. This also carries over to nations and corporations where hacking is a tool of social control used to gain power and disrupt political and economic systems (Burkart and McCourt 2019). Overall, it seems that hacking may serve as a means of re-asserting control over the environment. This leads us to look more closely at types of control, namely, primary and secondary control mechanisms, and how these are related to the dark traits in predicting hacker intent and behavior.

Primary and Secondary Control

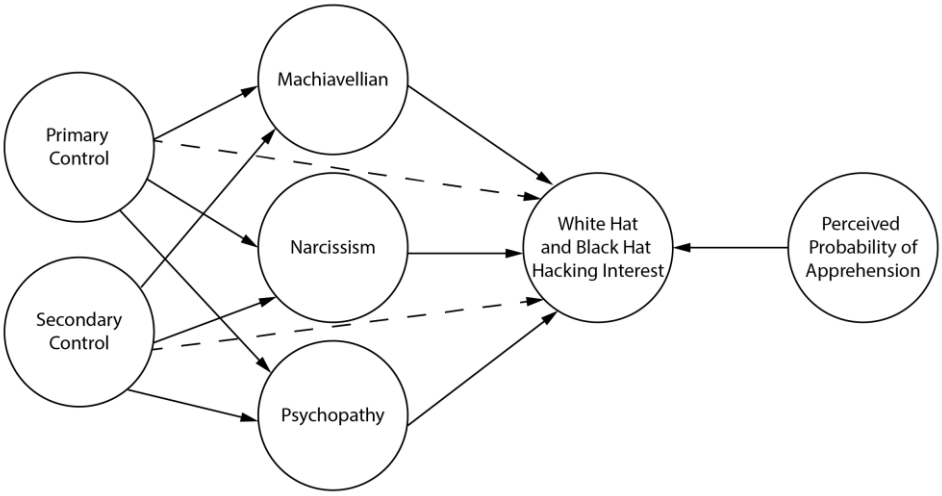
Primary control is related to the intrinsic need to control the environment and other people. In contrast, secondary control is an adaptive behavior providing enjoyment, gratification, and pleasure via positive thoughts and mood that helps the individual maintain the perception of control. To maintain feelings of control, individuals invoke different strategies, including (1) primary control, whereby individuals attempt to gain direct control by altering the environment to correspond to their wishes, and (2) secondary control, whereby individuals essentially alter themselves or align with environmental forces to create the perception of control. Both primary and secondary control are essential for coping with the environment. However, there is strong evidence from evolutionary, comparative, developmental, and cultural psychology that primary control underpins behavioral strategies throughout the individual's life and across cultures (Heckhausen and Schulz 1999). At the same time, secondary control strategies are necessary because individuals sometimes fail to achieve their goals and are required to be selective in the goals they pursue. When individuals experience failure and the loss of primary control, they adjust to the environment by moving towards a secondary control strategy (Heckhausen and Schulz 1992; Heckhausen and Schulz 1999).

Given the evidence that hackers report feeling a sense of control when engaging in successful hacking activities and existing researchers' speculations regarding the high need for control among hacking personas (Rennie and Shore 2007), we consider how the different control motivations align with the Dark Triad to predict different types of hacking intent and attitudes. Specifically, we assert that primary and secondary control will be related to the Dark Triad characteristics and, in turn, will lead to an interest in white hat and black hat hacking.

RESEARCH QUESTIONS AND HYPOTHESES

Figure 1 presents an overview of the significant questions examined in this paper. In this section, we detail the hypotheses related to the model.

FIGURE 1
RESEARCH MODEL



The first hypothesis involves a mediation analysis (Hair et al. 2022) on the role of the Dark Triad in mediating the effect of primary and secondary control on white and black hacking interests. Based on the previous discussion, we expect the Dark Triad to mediate the relationship between primary and secondary control and hacking interest. The implication is that the Dark Triad governs the nature of the relationship and, in turn, the underlying mechanism and progression between the control constructs and white hat and black hat hacking, thus prompting further investigation of these relationships.

H1: *Machiavellianism, narcissism, and psychopathy mediate the relationship between primary and secondary control and white hat and black hat hacking.*

To investigate these relationships further, we examine how primary and secondary control relates to dark traits. We hypothesize that high levels of primary control are related to higher levels on the Machiavellianism, narcissism, and psychopathy scales. There is evidence that the dark traits are related to higher perceptions of external locus of control (Aldousari et al. 2017), making it likely that these individuals would likewise have higher levels of primary control, as this is a survival strategy that is related to the intrinsic need to exert control over the environment and others. Hacking expertise coupled with opportunity facilitates environmental control. At the same time, secondary control strategies are necessary because primary control does not always help the individual achieve their goals and needs to sync with the environmental demands and move towards secondary control strategies. Based on the above argument, we propose the following hypothesis:

H2: *Higher levels of primary and secondary control are related to higher levels of Machiavellianism, narcissism, and psychopathy.*

Our last research question revalidates the role of psychological traits in being attracted to white hat and black hat hacking. White hat and black hat hackers may have manifestations of Machiavellianism, narcissism, and psychopathy, as suggested in existing work (e.g., Gaia 2020). We also draw on several prior studies investigating the relationship between computer abuse and crime as influenced by narcissism, Machiavellianism, and psychopathy as additional justification (Maasberg 2020; Nevin 2015; Seigfried-Spellar et al. 2017).

H3: *The Dark Triad, consisting of Machiavellianism, narcissism, and psychopathy, is positively related to interest in white and black hat hacking.*

RESEARCH METHODOLOGY

The references, scales, and loadings used in this study can be viewed at the following source (https://github.com/anonymousgroundhog/Wits). There is a brief overview of the scales in the Appendix. The *primary control* scale was derived from Dan et al. (Dan et al. 2011). The *secondary control* items were from Wrosch and Heckhausen (Wrosch and Heckhausen 1996) and Dan et al. (Dan et al. 2011). The *Dark Triad Dirty Dozen* measured the dark traits because it is concise and has been rigorously validated by several studies (Jonason and Luevano 2013; Jonason and Webster 2010; Webster and Jonason 2013). The scale's psychometric properties have also been validated for use in several cultures (Czarna et al. 2016; Jonason and Luevano 2013; Ozsoy et al. 2017; Savard et al. 2017). The *probability of being apprehended* construct was adapted from a study that identified the role of monetary incentives in violating HIPAA regulations and privacy laws. This study used responses to three scenarios to construct a latent variable labeled the *probability of being apprehended*, measuring the subject's perceived likelihood of being caught (Gaia et al. 2020). The validated white and black hat scales were from (Gaia 2020). The white hat scale measures the attraction to technical and social engineering hacking behaviors. The subjects completing the scale are told they would work for a government agency and would not be prosecuted for participating in white hat activities. The three black hat items involve financial attacks motivated by personal gains for breaching computer systems. These are the monetary incentives to engage in black hat hacking behavior. These activities are typically illegal.

DATA COLLECTION AND ANALYSIS

We recruited 593 subjects from sophomore, junior, and senior undergraduates enrolled in management information systems and a data analytics class at the University of Buffalo to take an online Qualtrics survey. The study was approved by the Institutional Review Board (IRB). The data was collected in March and April of 2022, and the final number of subjects used in the analysis was 523. We removed from the study any subjects missing more than 10% of the values or taking less than two minutes to complete the survey because speedy responses tend to introduce noise into the results.

Student populations provide a solid foundation for researching and investigating hacking insider activity for several reasons. First, students will be entering the workforce immediately and represent the emerging workforce. Secondly, students are less concerned with social desirability issues than existing employees because the survey was anonymous. Within organizations and work environments, subjects are less prone to answer questions truthfully because they do not want to diminish their social prestige (Akbulut et al. 2017; Dodou and de Winter 2014). In contrast to individuals from organizations and individuals with high-status jobs, we have found that students are less prone to over-report "good behavior" and under-report "bad behavior." As our results will show, rather than not engaging in illegal acts, approximately 56% of the subjects indicated they would receive money in times of monetary stress. All subjects who participated in the survey were advised to withdraw from participation at any time without penalty. Participants were given extra credit for participating in the study. We used SmartPLS 3.0 to perform partial least squares because it is robust, resistant to statistical inadequacies, and effective in handling complex multidimensional constructs (Henseler and Chin 2010). SmartPLS 3.0 effectively handles reflective sub-latent variables and prediction (Henseler 2018).

MEASUREMENT ASSESSMENT

We examined individual loadings and internal consistency to test for item reliability. Loadings for all measurement items were above 0.7. Table 1 illustrates that Cronbach's alpha for every construct was more significant than 0.7, indicating internal reliability (Werts et al. 1974). Next, we assessed discriminant

validity using the average variance extracted (AVE). The square root of the AVE should be higher than the correlations among the constructs. See Table 2 for the latent variable correlations for the white hat model.

TABLE 1
LATENT VARIABLE STATISTICS

Variables			
	Cronbach's Alpha	Composite Reliability	Average Variance Extracted
Primary Control	0.802	0.883	0.717
Secondary Control	0.874	0.922	0.798
Machiavellian	0.849	0.890	0.689
Narcissistic	0.791	0.865	0.616
Psychopathy	0.863	0.907	0.709
White hat	0.940	0.953	0.771
Black hat	0.917	0.947	0..857

TABLE 2
LATENT VARIABLE CORRELATIONS

		1.	2.	3	4	5.	6	7	8
1	**Machiavellian**	1	0.474	-0.204	0.342	0.576	-0.023	0.549	0.415
2	**Narcissism**	0.474	1	-0.05	0.389	0.309	0.087	0.326	0.187
3	**Perceived Probability**	-0.204	-0.05	1	-0.071	-0.211	-0.005	-0.276	-0.297
4	**Primary Control**	0.342	0.389	-0.071	1	0.199	0.132	0.24	0.166
5	**Psychopathy**	0.576	0.309	-0.211	0.199	1	-0.124	0.511	0.398
6	**Secondary Control**	-0.023	0.087	-0.005	0.132	-0.124	1	-0.061	-0.092
7	**White Hat**	0.549	0.326	-0.276	0.24	0.511	-0.061	1	0.627
8	**Black Hat**	0.415	0.187	-0.297	0.166	0.398	-0.092	0.627	1

RESEARCH MODEL AND HYPOTHESES ASSESSMENT

All of the hypotheses were analyzed using the SmartPLS package. One criterion for evaluating PLS path models is the r^2, or the *coefficient of determination*. According to Cohen (Cohen 1992), a small r^2 effect size is less than approximately 0.14, a medium effect size is between 0.14 and 0.26, and a large effect size is more significant than 0.26. The *p*-values follow the path coefficients on the connecting lines. Paths that are statistically significant at the .05 level are darker.

FIGURE 2
MEDIATION ANALYSIS WHITE HAT

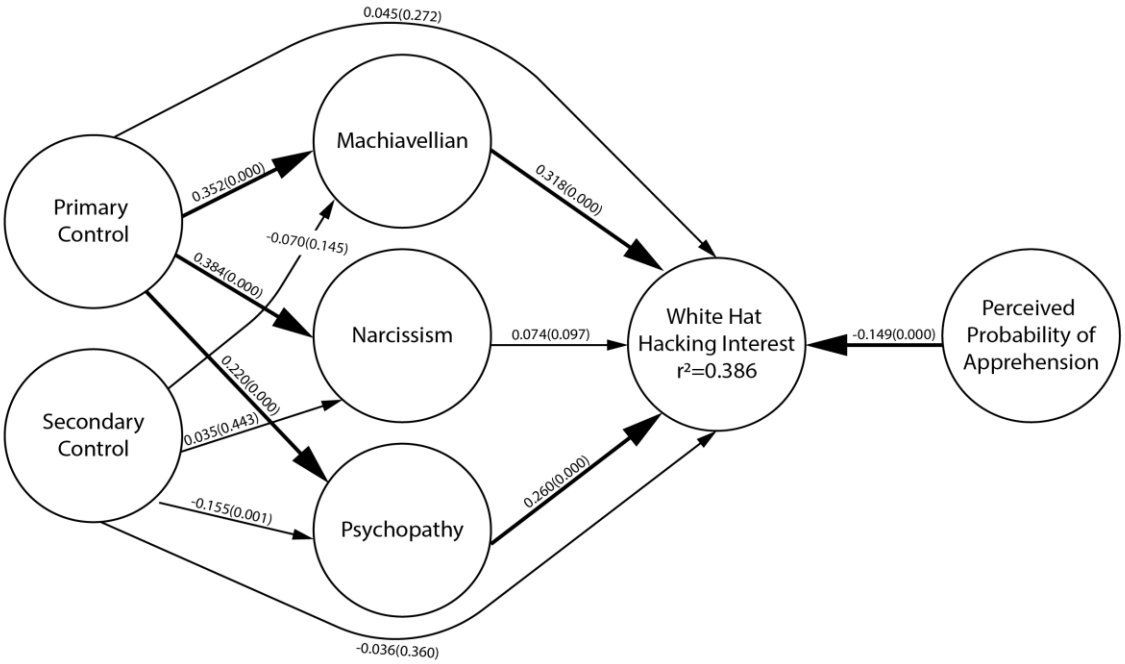
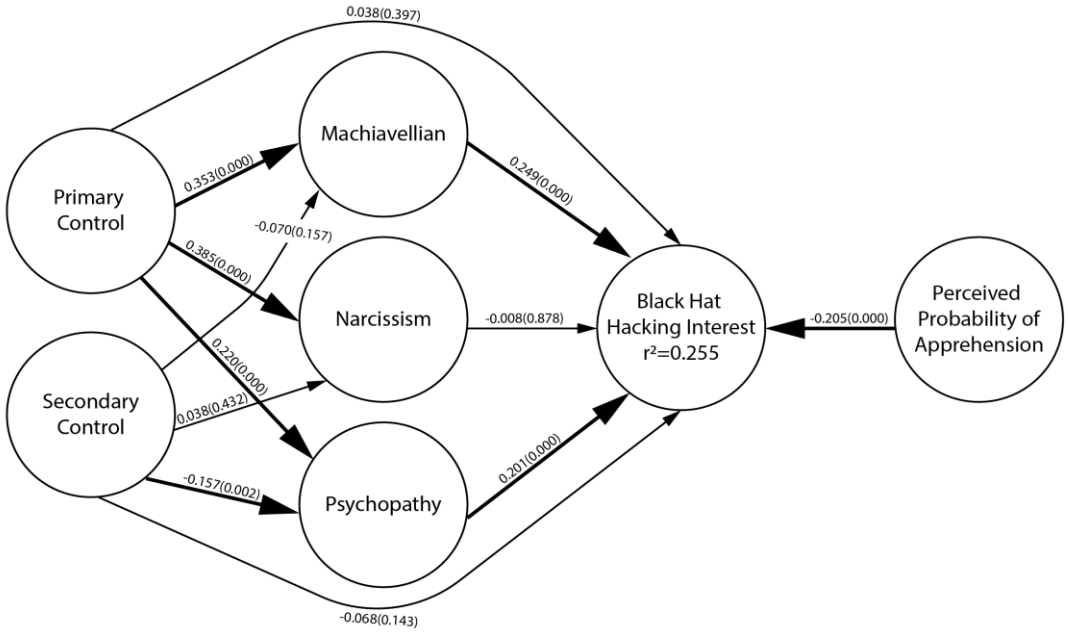


FIGURE 3
MEDIATION ANALYSIS FOR BLACK HAT



Overall, H1 was supported. Figures 2 and 3 present the models used to examine the mediation relationship. We included direct and indirect paths from the control constructs to the white hat and black constructs and used the dark triad as the mediator. The paths were run simultaneously, and the direct paths from the control constructs to white hat hacking were not statistically significant. However, the paths from

primary and secondary control to the dark traits were statistically significant, as well as the paths from the dark triad to the white hat and black hat hacking interest. According to (Hair et al. 2022), this is the best-case scenario because it suggests that our mediator, the Dark Triad, supports the hypothesized theoretical framework. The mediation results for the black hat model were essentially the same. The remaining hypotheses will be examined without the direct effects of primary and secondary control on the white and black hat constructs.

H2 was supported for primary control, see Figures 4 & 5, as the path coefficients from primary control to Machiavellianism, narcissism, and psychopathy were positive and statistically significant, $p < .05$. Primary control explained significant variance in Machiavellianism, narcissism, and psychopathy in both the white hat and black hat hacking models. However, there was no support for H2 in terms of secondary control. The paths from secondary control to Machiavellianism and narcissism were not statistically significant, and the path from secondary control to psychopathy was statistically significant but negative. However, upon reflection, secondary control and psychopathy have a negative relationship, which makes sense because individuals with high levels of secondary control alter themselves and align with environmental forces and others, which is the antithesis of psychopathy. The path coefficients may differ slightly for the white hat and black hat models (for example, 0.351 vs. 0.353) because of missing values.

Lastly, H3 was partially supported for two of the Dark Triad constructs. Machiavellianism and psychopathy were statistically significant predictors of white and black hat hacking. Interestingly, the path coefficient from narcissism to black and white hat hacking was not statistically significant.

FIGURE 4
RESULTS FOR WHITE HAT

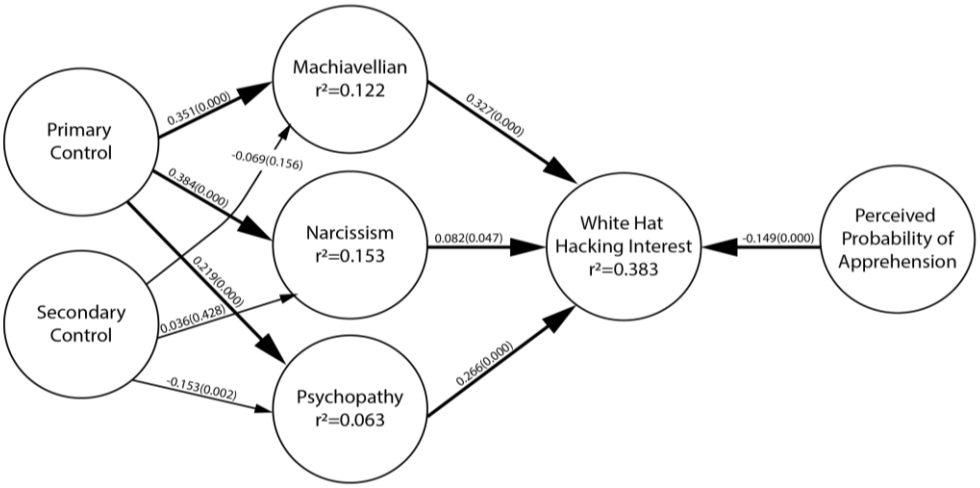
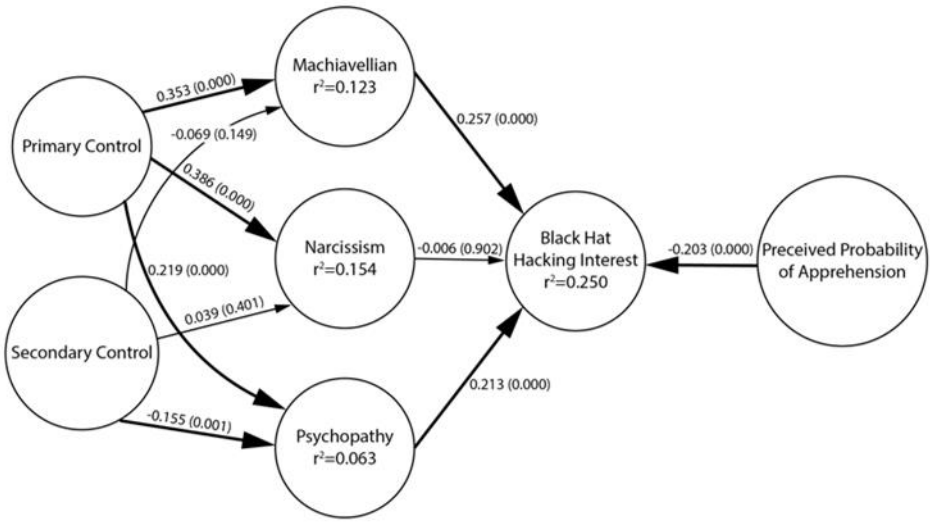


FIGURE 5
RESULTS FOR BLACK HAT



CONCLUSION AND FUTURE RESEARCH

Through the present study, we found further support for the importance of Machiavellianism, psychopathy, and the perceived probability of apprehension. These variables strongly predict interest in and desire to engage in white and black hat hacking. Primary control was also found to influence the Dark Triad moderately. Secondary control had a moderate negative effect on psychopathy.

In addition to these findings, we conducted a mediation analysis on the role of the Dark Triad in mediating the effect of primary and secondary control on white and black hacking interests (Hair et al., 2022). The preliminary results show that the Dark Triad mediates the relationship between primary and secondary control and hacking interest. The implication is that the Dark Triad governs the nature of the relationship and, in turn, the underlying mechanism and progression between the control constructs and white hat and black hat hacking, thus prompting further investigation of these relationships.

There is interest in developing a maliciousness index for identifying individuals with the potential to engage in unlawful hacking behavior using psychological testing (King et al., 2018). Subjects would likely subvert any such testing. However, there is potential for using primary control as a preliminary indicator and interest in white hat hacking as an indirect approach for engaging in black hat hacking.

Notwithstanding the difficulty of conducting insider research with actual employees, the next step will be to solicit such participation to increase the generalizability of the results.

ACKNOWLEDGMENT

This material is based upon work supported by the U.S. National Science Foundation under Grant No. DGE-1754085.

REFERENCES

Akbulut, Y., Donmez, A., & Dursun, O.O. (2017). Cyberloafing and Social Desirability Bias among Students and Employees. *Computers in Human Behavior*, *72*, 87–95.

Bertl, B., Pietschnig, J., Tran, U.S., Stieger, S., & Voracek, M. (2017). More or Less Than the Sum of Its Parts? Mapping the Dark Triad of Personality onto a Single Dark Core. *Personality and Individual Differences*, *114*, 140–144.

Burkart, P., & McCourt, T. (2019). *Why Hackers Win: Power and Disruption in the Network Society*. Oakland, California: University of California Press.

Chickowoski, E. (2018). *The 6 Worst Insider Attacks of 2018 – So Far*. Retrieved June 12, 2019, from https://www.darkreading.com/the-6-worst-insider-attacks-of-2018---so-far/d/d-id/1332183?image_number=7

Cohen, J. (1992). A Power Primer. *Psychological Bulletin*, *112*(1), 155–159.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future Directions for Behavioral Information Security Research. *Computers & Security*, *32*, 90–101.

Czarna, A.Z., Jonason, P.K., Dufner, M., & Kossowska, M. (2016). The Dirty Dozen Scale: Validation of a Polish Version and Extension of the Nomological Net. *Frontiers in Psychology*, *7*.

Dan, O., Sagi-Schwartz, A., Bar-haim, Y., & Eshel, Y. (2011). Effects of Early Relationships on Children's Perceived Control: A Longitudinal Study. *International Journal of Behavioral Development*, *35*(5), 449–456.

Dhillon, G., Samonas, S., & Etudo, U. (2016). Developing a Human Activity Model for Insider Is Security Breaches Using Action Design Research. *Ict Systems Security and Privacy Protection, Sec 2016*, *471*, 49–61.

Dodou, D., & de Winter, J.C.F. (2014). Social Desirability Is the Same in Offline, Online, and Paper Surveys: A Meta-Analysis. *Computers in Human Behavior*, *36*, 447–495.

Gaia, J., Ramamurthy, B., Sanders, G.L., Sanders, S.P., Upadhyaya, S., Wang, X., & Yoo, C.W. (2020). Psychological Profiling of Hacking Potential. *Hawaii International Conference on Systems Sciences*, Maui, Hawaii.

Gaia, J., Sanders, G.L., Sanders, S.P., Upadhyaya, S., Wang, X., & Yoo, C.W. (2021). Dark Traits and Hacking Potential. *Journal of Organizational Psychology*, *21*(3).

Gaia, J., Wang, X.Y., Yoo, C.W., & Sanders, G.L. (2020). Good News and Bad News About Incentives to Violate the Health Insurance Portability and Accountability Act (Hipaa): Scenario-Based Questionnaire Study. *Jmir Medical Informatics*, *8*(9), e15880.

Hair, J.F., Hult, G.T.M., Ringle, C.M., & Sarstedt, M. (2022). *A Primer on Partial Least Squares Structural Equation Modeling (Pls-Sem)* (3rd Ed.). Los Angeles: SAGE.

Heckhausen, J. (2006). *Developmental Regulation in Adulthood: Age-Normative and Sociostructural Constraints as Adaptive Challenges*. New York, NY: Cambridge University Press.

Heckhausen, J., & Schulz, R. (1992). Shifting Preferences for Primary and Secondary Control across the Life Course - A New Conceptualization. *Ceskoslovenska Psychologie*, *36*(1), 1–9.

Heckhausen, J., & Schulz, R. (1999). The Primacy of Primary Control Is a Human Universal: A Reply to Gould's (1999) Critique of the Life-Span Theory of Control. *Psychological Review*, *106*(3), 605–609.

Henseler, J. (2018). Partial Least Squares Path Modeling: Quo Vadis? *Quality & Quantity*, *52*(1), 1–8.

Henseler, J., & Chin, W.W. (2010). A Comparison of Approaches for the Analysis of Interaction Effects between Latent Variables Using Partial Least Squares Path Modeling. *Structural Equation Modeling-a Multidisciplinary Journal*, *17*(1), 82–109.

Hijji, M., & Alam, G. (2021). A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the Covid-19 Pandemic: Challenges and Prospective Solutions. *IEEE Access*, *9*, 7152–7169.

Jonason, P.K., & Luevano, V.X. (2013). Walking the Thin Line between Efficiency and Accuracy: Validity and Structural Properties of the Dirty Dozen. *Personality and Individual Differences*, *55*(1), 76–81.
Jonason, P.K., & Webster, G.D. (2010). The Dirty Dozen: A Concise Measure of the Dark Triad. *Psychological Assessment*, *22*(2), 420–432.
Jones, D.N., Padilla, E., Curtis, S.R., & Kiekintveld, C. (2021). Network Discovery and Scanning Strategies and the Dark Triad. *Computers in Human Behavior*, *122*.
Kajtazi, M., Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2014). Assessing Sunk Cost Effect on Employees' Intentions to Violate Information Security Policies in Organizations. *47th Hawaii International Conference on System Sciences (Hicss)*, pp. 3169–3177.
King, Z.M., Henshel, D.S., Flora, L., Cains, M.G., Hoffman, B., & Sample, C. (2018). Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment. *Frontiers in Psychology*, *9*.
Krit, S.D., & Haimoud, E. (2016). Review on the It Security Attack and Defense. *2016 International Conference on Engineering & Mis (Icemis)*.
Maasberg, M., Van Slyke, C., Ellis, S., & Beebe, N. (2020). The Dark Triad and Insider Threats in Cyber Security. *Communications of the ACM*, *63*(12), 64–80.
Muris, P., Merckelbach, H., Otgaar, H., & Meijer, E. (2017). The Malevolent Side of Human Nature: A Meta-Analysis and Critical Review of the Literature on the Dark Triad (Narcissism, Machiavellianism, and Psychopathy). *Perspectives on Psychological Science*, *12*(2), 183–204.
Nevin, A.D. (2015). Cyber-Psychopathy: Examining the Relationship between Dark E-Personality and Online Misconduct. In *The School of Graduate and Postdoctoral Studies*. The University of Western Ontario.
Ozsoy, E., Rauthmann, J.F., Jonason, P.K., & Ardic, K. (2017). Reliability and Validity of the Turkish Versions of Dark Triad Dirty Dozen (Dtdd-T), Short Dark Triad (Sd3-T), and Single Item Narcissism Scale (Sins-T). *Personality and Individual Differences*, *117*, 11–14.
Palmer, C.C. (2001). Ethical Hacking. *IBM Systems Journal*, *40*(3), 769–780.
Paulhus, D.L., & Williams, K.M. (2002). The Dark Triad of Personality: Narcissism, Machiavellianism, and Psychopathy. *Journal of Research in Personality*, *36*(6), 556–563.
Pelster, M., Hofmann, A., Klocke, N., & Warkulat, S. (2021). Dark Triad Personality Traits and Selective Hedging. *Journal of Business Ethics*.
Pranggono, B., & Arabo, A. (2021). Covid-19 Pandemic Cybersecurity Issues. *Internet Technology Letters*, *4*(2).
Rennie, L., & Shore, M. (2007). An Advanced Model of Hacking. *Security Journal*, *20*(4), 236–251.
Robert Willison, P.B.L., & Paternoster, R. (2018). A Tale of Two Deterrents: Considering the Role of Absolute and Restrictive Deterrence to Inspire New Directions in Behavioral and Organizational Security Research. *Journal of the Association for Information Systems*.
Roy Sarkar, K. (2010). Assessing Insider Threats to Information Security Using Technical, Behavioural and Organisational Measures. *Information Security Technical Report*, *15*(3), 112–133.
Safa, N.S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and Opportunity Based Model to Reduce Information Security Insider Threats in Organisations. *Journal of Information Security and Applications*, *40*, 247–257.
Savard, C., Simard, C., & Jonason, P.K. (2017). Psychometric Properties of the French-Canadian Version of the Dark Triad Dirty Dozen. *Personality and Individual Differences*, *119*, 122–128.
Seigfried-Spellar, K.C., Villacis-Vukadinovic, N., & Lynam, D.R. (2017). Computer Criminal Behavior Is Related to Psychopathy and Other Antisocial Behavior. *Journal of Criminal Justice*, *51*, 67–73.
Silic, M., & Lowry, P.B. (2021). Breaking Bad in Cyberspace: Understanding Why and How Black Hat Hackers Manage Their Nerves to Commit Their Virtual Crimes. *Information Systems Frontiers*, *23*(2), 329–341.
Warkentin, M., Vance, A., & Johnston, A.C. (2016). Introduction to the Hicss-49 Minitrack on Innovative Behavioral Is Security and Privacy Research. *Proceedings of the 49th Annual Hawaii International Conference on System Sciences (HICSS 2016)*, pp. 3635–3635.

Webster, G.D., & Jonason, P.K. (2013). Putting the "Irt" in "Dirty": Item Response Theory Analyses of the Dark Triad Dirty Dozen-an Efficient Measure of Narcissism, Psychopathy, and Machiavellianism. *Personality and Individual Differences*, *54*(2), 302–306.
Werts, C.E., Linn, R.L., & Joreskog, K.G. (1974). Intraclass Reliability Estimates - Testing Structural Assumptions. *Educational and Psychological Measurement*, *34*(1), 25–33.
Weston, S. (2020). *Insider Data Breaches Set to Increase Due to Remote Work Shift*.
White, R.W. (1959). Motivation Reconsidered - The Concept of Competence. *Psychological Review*, *66*(5), 297–333.
Wrosch, C., & Heckhausen, J. (1996). Adaptiveness of Social Comparisons: Developmental Regulation Via Primary and Secondary Control. *Zeitschrift Fur Entwicklungspsychologie Und Padagogische Psychologie*, *28*(2), 126–147.
Wrosch, C., Heckhausen, J., & Lachman, M.E. (2000). Primary and Secondary Control Strategies for Managing Health and Financial Stress across Adulthood. *Psychology and Aging*, *15*(3), 387–399.

APPENDIX: SURVEY ITEMS

Example of Probability of Apprehension Items **What do you think is the likelihood of getting caught, if you accept the money?**
Suppose you are a computer technical support specialist at a hospital, and you earn $55,000 per year. However, you are currently experiencing financial difficulty. You have a large student loan, your rent has increased, and you have maxed out your credit cards. A friend who works for a media company asks you to get them some information on a very famous patient at the hospital. What amount of money would you receive to make this acceptable?

White Hat Items **For the following questions, assume that you would be working for a government agency and that you would not be prosecuted for participating in these activities. Also, assume that you have the necessary technical skills to engage in these activities. Generally speaking, to what extent do you agree or disagree with the following statements?**
I would like to pretend I am an authority figure to obtain a password.
I would like to observe a person's behavioral patterns over a week and use that as a way to obtain their personal information.
I would like to use manipulative emails to obtain private information or install malware on computers.
I would like to sneak into buildings using a lock pick, by following someone else, or by using an electronic device to counter the lock system.
I would like to use password crackers to break into computer accounts.
I would like to set up a website that looks like a real website to trick people into entering their personal information.

Black Hat Items **For the following questions, assume that you would not get caught for participating in the following activities and that you have the necessary technical skills to engage in these activities. Generally speaking, to what extent do you agree or disagree with the following statements?**
I could see myself engaging in hacking attacks if I needed money to purchase a $400,000 house for my family.
I could see myself engaging in hacking attacks if I needed money to purchase a new $60,000 car that I could not afford.
I could see myself engaging in hacking attacks if I needed money to pay off a credit card debt that had reached $100,000 and I was just fired from my job.

Dark Triad and Control Items Generally speaking, to what extent do you agree or disagree with the following statements?	
Machiavellian	I have used deceit or lied to get my way.
Machiavellian	I tend to manipulate others to get my way.
Machiavellian	I have used flattery to get my way.
Machiavellian	I tend to exploit others towards my own end.
Narcissism	I tend to want others to admire me.
Narcissism	I tend to want others to pay attention to me.
Narcissism	I tend to expect special favors from others.
Narcissism	I tend to seek prestige or status.
Psychopathy	I tend to lack remorse.
Psychopathy	I tend to be callous or insensitive.
Psychopathy	I tend to be unconcerned with the morality of my actions.
Psychopathy	I tend to be cynical.
Primary Control	When my friends think differently than me, I will convince them that I am right.
Primary Control	I insist on my right to explain what I want, until others understand me.
Primary Control	When I don't agree with others, I will try to convince them that I am right.
Secondary Control	Even when I can't change a bad situation, I can find good things in it and feel better.
Secondary Control	Even when everything seems to be going wrong, I can usually find a bright side to the situation.
Secondary Control	I can find something positive, even in the worst situations.